(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 949 788 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
13.10.1999 Bulletin 1999/41

(51) Int. Cl.[6]: **H04L 29/06**, H04L 12/22, G06F 1/00

(21) Application number: **98410038.8**

(22) Date of filing: **10.04.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant:
SUN MICROSYSTEMS, INC.
Mountain View, California 94043-1100 (US)

(72) Inventors:
- **Ares Blanco, Marcos**
  38100 Grenoble (FR)
- **Marco, Régis**
  38240 Meylan (FR)

(74) Representative:
de Beaumont, Michel
1, rue Champollion
38000 Grenoble (FR)

(54) Network access authentication system

(57) A network access authentication system including a directory service containing a remote access password and a standard access password for each user of the network, using an authentication protocol that provides information on whether a user is accessing the network locally or remotely, and including a front-end between the directory service and the authentication protocol. The front-end executes the steps of:

receiving a user identifier and a user password entered by a user through said authentication protocol;

retrieving from the directory service the remote access password and the standard access password corresponding to the user identifier;

if the authentication protocol indicates a remote access, comparing the user password to the remote access password, else comparing the user password to the standard access password; and

granting access to the network if the comparing step is successful.

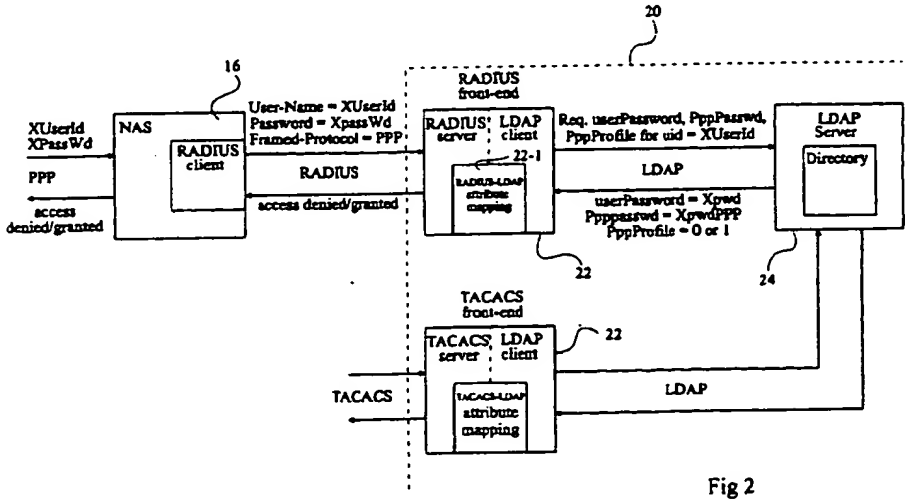

Fig 2

EP 0 949 788 A1

Printed by Xerox (UK) Business Services
2.16.7/3.6

tion with the directory service using the directory service protocol, LDAP in the preferred embodiment. Moreover, the front-end behaves as the server for the clients using the corresponding authentication protocol. As shown, a NAS (network access server) 16 runs a RADIUS client which will exchange authentication information with the corresponding front-end 22 by using the RADIUS protocol. Remote clients connect to the NAS 16 using, for example, the Point-to-Point Protocol (PPP).

[0030] The front-ends 22 are, in a preferred embodiment, implemented within the computer 20 hosting the directory service. They can however be implemented in other computers connected to the network.

[0031] The directory is maintained by an administrator using a conventional LDAP client (shown in Figure 1).

[0032] When a remote user wishes to access the network, he provides a user identifier XUserId and a password XPassWd. This information is passed to the RADIUS client application which conventionally carries out a RADIUS authentication transaction with the available RADIUS server, i.e. the RADIUS front-end according to the invention.

[0033] According to the RADIUS protocol, like for other high-level protocols such as TACACS and LDAP, information is exchanged in the form of attributes. Each attribute has a unique attribute identifier and an attribute value.

[0034] During the RADIUS authentication transaction, the client will in particular pass to the RADIUS server the attributes "User-Name" with the value XUserId (the user identifier entered by the remote user), the attribute "Password" with the value XPassWd (the password entered by the remote user), and the attribute "Framed-Protocol" with a value indicating if a remote access protocol is used and if so, which one (in this case PPP). In practice, the password XPassWd will be encrypted on the PPP link and decrypted by the NAS 16. The RADIUS client will again encrypt the password conforming to the RADIUS specifications.

[0035] The RADIUS server needs to compare the user identifier and the password with predefined values which, in a conventional system, are stored in a dedicated file. According to the invention, the front-end's RADIUS server, instead of retrieving this data in a file, will make the front-end's LDAP client fetch it from the directory service 24. For this purpose, the front-end converts the required RADIUS attributes to LDAP attributes using an attribute mapping table 22-1. In particular, the RADIUS attribute "User-Name" is mapped to the LDAP attribute "uid". The LDAP client then conventionally issues a request to the LDAP server for data associated to attribute "uid" having value XUserId (the user identifier). The LDAP server conventionally returns the requested attributes with their corresponding values stored in the directory.

[0036] In figure 2, the requested attributes are, for example, "userPassword", which is a password to use for local or standard accesses, "PppPassWd" which is a password to use normally for remote accesses, and "PppProFile" which is a flag that indicates if the user should use his remote access password or not when using a remote access. Depending on the values of these attributes and those received from the RADIUS client, the front-end's RADIUS server will either deny or grant access to the network.

[0037] Figure 3 shows an exemplary flow chart of the operations carried out by the RADIUS front-end of figure 2 when a user wishes to access the network remotely.

[0038] At 100, the front-end receives from the RADIUS client the attributes corresponding to the user identifier XUserId, the entered password XPassWd, and the type of the remote access protocol, PPP. The two first values are provided by the user, whereas the third value is provided by the RADIUS client which is aware of the type of remote access protocol used.

[0039] At 102, the RADIUS attribute "User-Name" is mapped to the LDAP attribute "uid" with the user identifier value XUserId. An LDAP request is then issued to retrieve from the directory the attributes "userPassword", "PppPassWd" and "PppProFile" from an entry corresponding to value XUserId for attribute "uid".

[0040] At 104, if the LDAP server cannot satisfy the request because no entry corresponds to XUserId, the access to the network is denied at 106. Else, at 108, the value the "Framed-Protocol" attribute is checked.

[0041] If at 108 the "Framed-Protocol" attribute indicates a PPP access, it is checked whether the "PppProfile" flag is zero at 114. The "PppProfile" flag is optional and allows the administrator to force a user either to always use the same password, i.e. the standard access password, whether he is accessing the network remotely or not, or to force the user to use different passwords depending on the access mode.

[0042] If the "PppProfile" attribute is not zero at 114, the password XPassWd entered by the user is compared to the value of attribute "PppPassWd" at 116. If the comparison fails, access is denied at 106. Otherwise, access is granted at 112.

[0043] If the "PppProfile" attribute is zero at 114, the password XPassWd entered by the user is compared at 118 to the value of attribute "userPassword" returned by the LDAP server. If the comparison fails, access is denied at 106, whereas, if it is successful, access is granted at 112.

[0044] If, at 108, the "Framed-Protocol" attribute does not indicate a PPP access, the same steps as carried out for the PPP access mode from 114 are carried out at 120 for any other possible access mode identified by the "Framed-Protocol" attribute. For example, if another possible remote access mode is SLIP, an enable flag "SlipProfile" and a password attribute "SlipPassWd" may be set for the user in the directory. The values of these attributes are compared respectively to zero and to the password XPassWd at steps similar to steps 114

and 116. Access is then granted or denied at steps similar to 112 or 106 if the flag "SlipProfile" is non zero.

[0045] If flag "SlipProfile" is zero or if no remote access mode is identified, the password XPassWd is compared to the value of attribute "userPassword" at 118 before granting or denying access.

[0046] It is apparent from the flowchart of figure 3 that an administrator may set at least two different passwords for a user in the directory. The administrator may force the user to use different passwords depending on the access mode (local or remote) and thus improve the security of the network. This feature may be overridden if the administrator sets the "PppProfile" attribute to 0. The user will then only use one password independently of the access mode, which may improve his comfort.

[0047] Provided that the system according to the invention has a front-end for each authentication protocol used on the network, it allows each user to have a single user identifier and a reduced number of passwords usable for any access or service on the network needing an authentication. The security of the network is improved when the administrator forces the user to have two passwords, one for local accesses, the other for remote accesses. An advantage of the system is that different front-ends may share the same password (PppPassWd, SlipPassWd) for the same access mode (PPP, SLIP).

[0048] User entries in the directory are customized for the needs of the invention, i.e. they have specific attributes which are not necessarily defined in existing directories. Directory service protocols, such as LDAP, are extensible in that an administrator may define new entry types in the directory, which entries may inherit attributes from pre-existing entry types or have newly defined attributes.

[0049] With LDAP, each entry of the directory is an instance of an "object class". An object class defines the attributes which must be used and the attributes which may be used in a corresponding entry. In this manner, new entry types may be added to the directory, transparently, provided that the LDAP client and the LDAP server both use the same object class definitions. An LDAP object class definition for user entries having the attributes exemplified above would be:

```
objectclass RemoteUser
  superior top
  requires
       uid
  allows
       userPassword
       PppPassWd,
       PppProFile,
       SlipPassWd,
       SlipProfile,
       ...
```

[0050] The statement "superior top" indicates that the object class inherits from the attributes of a previously defined object class "top". The statement "requires" is followed by a list of attributes that all the corresponding entries of the directory must have. The statement "allows" is followed by a list of attributes which are optional.

[0051] An instance of this object class, i.e. a corresponding entry in the directory, could be defined as follows:

```
dn: uid = XUserId, l = ?, o = ?, c = ?
objectclass = RemoteUser
uid = XUserId
userPassword = XPassWd
PppPassword = XPassWd2
PppProfile = 1.
```

[0052] The statement "dn:" defines the "distinguished name" which is a unique identifier for the entry. This distinguished name is defined so that the entries are organized hierarchically. For example, it defines the country "c", the organization "o", the location or city "l", and finally the user "uid". The statement "objectclass = RemoteUser" identifies the object class to which the entry belongs.

[0053] For ease of comprehension, only a limited number of attributes have been described, allowing a minimum authentication procedure. In practice, authentication procedures use more attributes, such as password expiration dates, check information, encryption keys, information for logging and debugging purposes... Those skilled in the art will add such attributes to the entries and object classes of a directory service and build the corresponding mapping tables in the front-ends for the various protocols which may be used for authentication.

Claims

1. A network access authentication system including:

   a directory service (24) containing a remote access password and a standard access password for each user of the network;
   an authentication protocol that provides information on whether a user is accessing the network locally or remotely; and
   a front-end (22) between the directory service and the authentication protocol, for receiving a user identifier and a user password entered by a user through said authentication protocol, retrieving from the directory service the remote access password and the standard access password corresponding to the user identifier, and granting access to the network when the authentication protocol indicates a remote access and the user password equals the remote access password, or when the authentication protocol indicates a local access and the user password equals the standard access password.

2. A network access authentication system including:

   a directory service (24) containing a remote access password, a standard access password, and a remote access password enable flag for each user of the network;
   an authentication protocol that provides information on whether a user is accessing the network locally or remotely; and
   a front-end (22) between the directory service and the authentication protocol for receiving a user identifier and a user password entered by a user through said authentication protocol, retrieving from the directory service the remote access password, the standard access password, and the remote access password enable flag corresponding to the user identifier, and granting access to the network if the authentication protocol indicates a remote access, the remote access enable flag has an active state, and the user password equals the remote access password, else if the authentication protocol indicates a local access or the remote access enable flag has an inactive state, and the user password equals the standard access password.

3. The authentication system of claim 1 or 2, wherein the front-end is a client for a protocol used by the directory service and a server for the authentication protocol, and includes a protocol attribute translation table for exchanging information between the authentication protocol and the directory service protocol.

4. The authentication system of claim 1 or 2, wherein the directory service uses the Lightweight Directory Access Protocol (LDAP), whereby each entry in the directory service is an instance of a predefined object class defining attributes which are used by the entry, a specific object class being created for the network users, that defines the attributes necessary for authenticating the users.

5. The authentication system of claim 1 or 2, wherein the front-end is an application executed on a computer hosting the directory service.

6. The authentication system of claim 1 or 2, including several authentication protocols and one front-end for each authentication protocol.

7. A network access authentication method using a directory service (24) containing a remote access password and a standard access password for each user of the network, including the steps of:

   receiving (100) a user identifier and a user password entered by a user through an authentication protocol that provides information on whether the user is accessing the network locally or remotely;
   retrieving (102) from the directory service the remote access password and the standard access password corresponding to the user identifier;
   if the authentication protocol indicates a remote access, comparing (116) the user password to the remote access password, else comparing (118) the user password to the standard access password; and
   granting access (112) to the network if the comparing step is successful.

8. A network access authentication method using a directory service containing a remote access password, a standard access password, and a remote access password enable flag for each user of the network, including the steps of:

   receiving (100) a user identifier and a user password entered by a user through an authentication protocol that provides information on whether the user is accessing the network locally or remotely;
   retrieving (102) from the directory service the remote access password, the standard access password, and the remote access password enable flag corresponding to the user identifier;
   if the authentication protocol indicates a remote access and the remote access enable flag has

an active state, comparing (116) the user password to the remote access password, else comparing (118) the user password to the standard access password; and

granting access (112) to the network if the comparing step is successful.

9. A network access authentication system including:

a directory service (24) containing a remote access password and a standard access password for each user of the network;
means (22) for receiving a user identifier and a user password entered by a user through an authentication protocol that provides information on whether the user is accessing the network locally or remotely;
means for retrieving from the directory service the remote access password and the standard access password corresponding to the user identifier;
means for comparing the user password to the remote access password if the authentication protocol indicates a remote access, else the user password to the standard access password; and
means for granting access to the network if the means for comparing indicate an equality.

10. A network access authentication system including:

a directory service (24) containing a remote access password, a standard access password, and a remote access password enable flag for each user of the network;
means (22) for receiving a user identifier and a user password entered by a user through an authentication protocol that provides information on whether the user is accessing the network locally or remotely;
means for retrieving from the directory service the remote access password, the standard access password, and the remote access password enable flag corresponding to the user identifier;
means for comparing the user password to the remote access password if the authentication protocol indicates a remote access and the remote access enable flag has an active state, else the user password to the standard access password; and
means for granting access to the network if the means for comparing indicate an equality.

11. The authentication system of claim 9 or 10, wherein said means for receiving, retrieving, comparing and granting access are included in a front-end (22) which is a client for a protocol used by the directory service and a server for the authentication protocol, and which includes a protocol attribute translation table (22-1) for exchanging information between the authentication protocol and the directory service protocol.

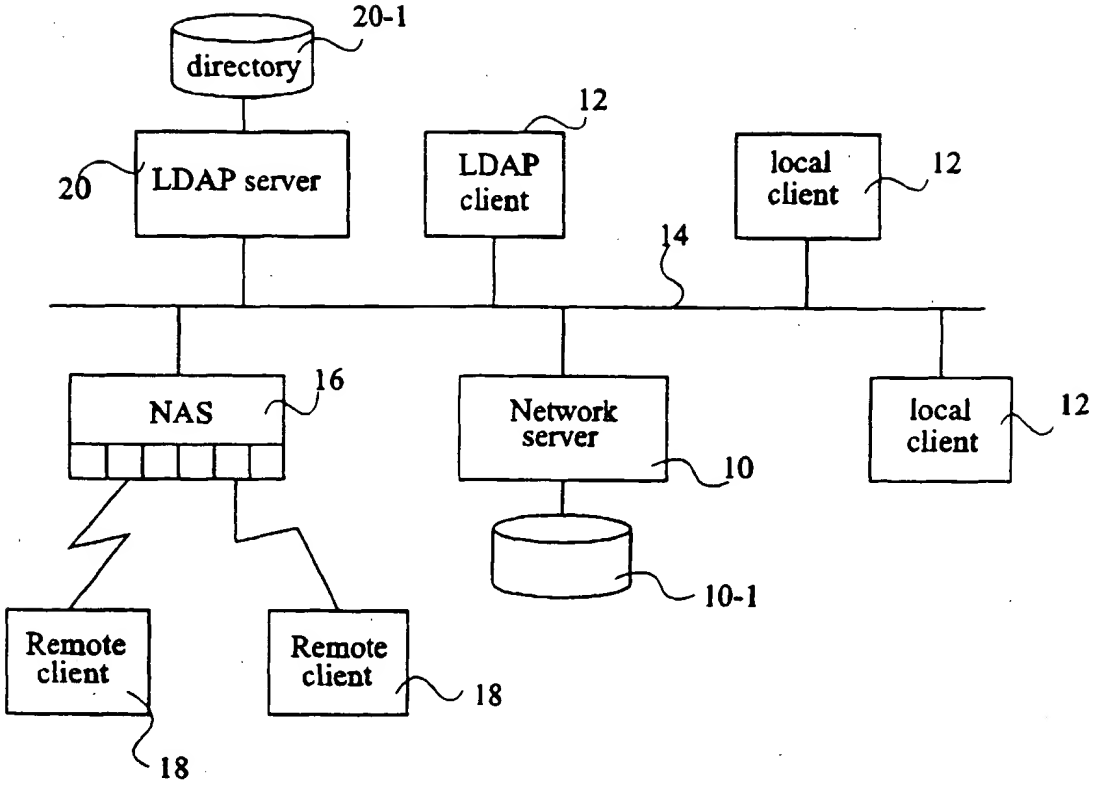

Fig 1

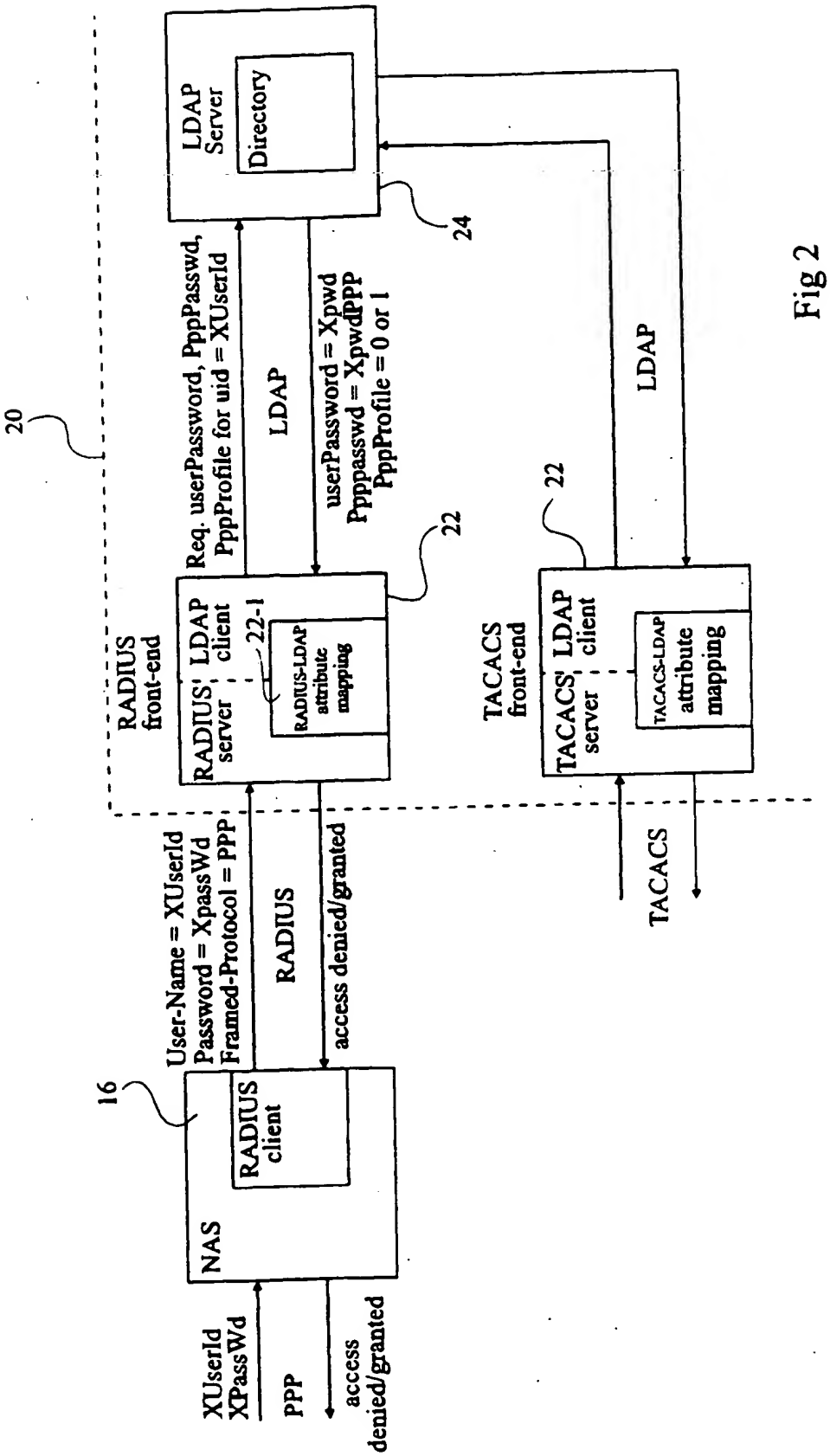

Fig 2

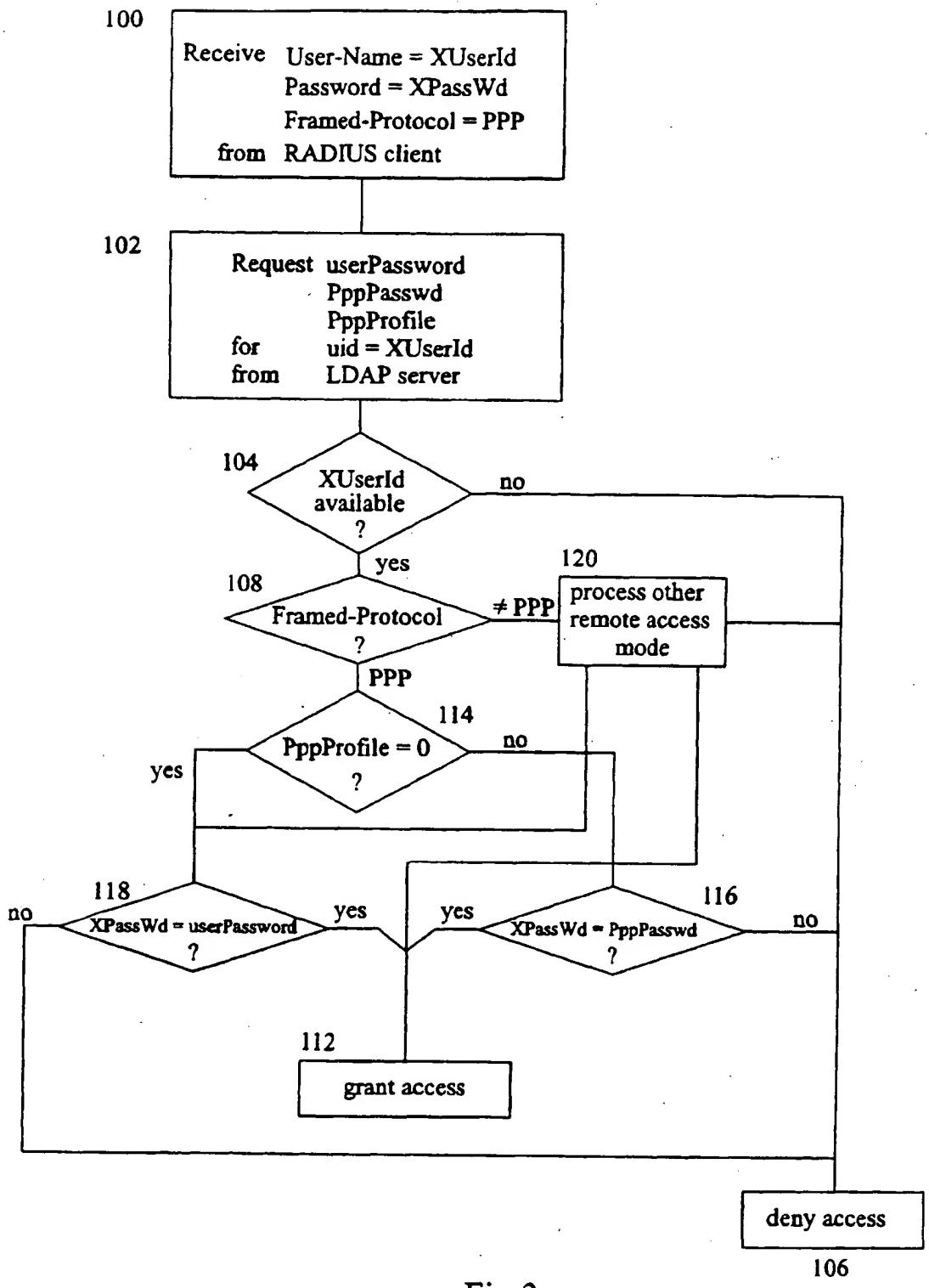

Fig 3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 41 0038

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	US 5 455 953 A (RUSSELL EDWARD A) 3 October 1995 * abstract * * column 3, line 3 - column 4, line 14 * * claims 1-6; figure 7 *	1-5,7-11	H04L29/06 H04L12/22 G06F1/00
A	US 5 586 260 A (HU WEI-MING) 17 December 1996 * column 1, line 44 - column 2, line 50; figure 1 *	1-11	
A	US 5 434 918 A (KUNG KENNETH C ET AL) 18 July 1995 * column 1, line 45 - line 56 * * column 3, line 15 - line 29; figure 1 *	1-3,5. 7-10	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

H04L
G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	8 September 1998	Karavassilis, N

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 41 0038

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

08-09-1998

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5455953 A	03-10-1995	CA 2102743 A	04-05-1995
US 5586260 A	17-12-1996	NONE	
US 5434918 A	18-07-1995	AU 676107 B	27-02-1997
		AU 1261595 A	03-07-1995
		CA 2153879 A	22-06-1995
		EP 0683907 A	29-11-1995
		JP 8502847 T	26-03-1996
		NO 953143 A	10-08-1995
		WO 9516947 A	22-06-1995

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82